FAA Low Risk NAS Application System

Security Function Protection Profile

Originating Organization: AIO-4

Date Issued: 1/28/04

Version Number: 1.0

Document Control Number: AIO-4-PP-LRNASAPS1.0

Conventions Used in this PP

Global

green text	FAA use

Section 3 Security Environment

Ax	assumption identifier
Tx	threat identifier
PGx	organizational security policy (OSP) identifier

Section 4 Security Objectives

Ox	security objective identifier

Section 5 Element Operations

+	iteration
blue text	assignment
purple text	selection

Contents

Exhibits

1
Introduction

This section identifies the nature, scope, and status of the FAA Low Risk NAS Application System Security Function.

1.1 Identification

1.1.1 Name: Federal Aviation Administration (FAA) Low Risk NAS Application System Security Function.

1.1.2 Identifier: Federal Aviation Administration (FAA) Low Risk NAS Application System Security Function], version 1.0, 1/28/04.

1.1.3 Keywords: FAA, National Airspace System (NAS), wide area network (WAN), local area network (LAN)/facility communications, end-user application system, security enclave

1.1.4 EAL: the EAL for this system is defined in Section 5.2 of this PP as EAL 2 augmented.

1.1.5 Evaluation Status: This Protection Profile has been subjected to an informal CCTL evaluation as part of the FAA internal review and approval process. It is currently undergoing formal CCTL evaluation.

1.2 Overview

This document specifies the security functional requirements and the security assurance requirements for the FAA Low Risk NAS Application System Security Function.

1.2.1 Overview

The Low Risk Application System Security Function is responsible for controlling, performing, and monitoring all security functions within an application system. The Low Risk Application System Security Function acts as the security kernel for an application system. Accordingly, the logical and physical boundaries of the TSF, TSC, and TOE are identical.

1.2.2 Strength of Function (SOF)

This is a low risk/routine system; accordingly the TOE SOF is basic.

1.2.3 Related PPs and Referenced Documents

The following references were consulted during the development of this Protection Profile, are referenced herein, or provide additional background information.

General

1. ACP-300-99-001, FAA Policy Memorandum, Safeguarding and Control of Sensitive Security Information (SSI), 30 November 1998.

2. ATS-SEC-01-001, FAA Policy Memorandum, Safeguarding and Control of Classified and Sensitive Information, dated January 2002.

3. DOT Handbook DOT H 1350.2, Departmental Information Resources Management Manual (DIRMM).

4. FAA, National Airspace System Architecture, Version 4.0 (or most recent version), January 1999.

5. FAA Order N1370.42, Password Management in the FAA, March 20, 2003.

6. FAA Order 1370.82, Information Systems Security Program, dated 6/9/00 (or more recent version).

7. FAA Order 1370.89, Information Operations Conditions, August 2003.

8. FAA Order 1600.2, Safeguarding Controls and Procedures for Classified National Security Information and Sensitive Unclassified Information.

9. FAA Order 1600.69, FAA Facilities Security Management Program.

10. FAA Order 1600.6, FAA Physical Security Management Program.

11. FAA Order 1600.1D, Personnel Security Program.

12. FAA Order 1600.72, Contractor and Industrial Security Program, April 4, 2001.

13. FAA Information System Security Enhancement Program Handbook, version 3 (or most current version).

14. ISO/IEC 15408-1 Information Technology - Security Techniques - Evaluation Criteria for IT, Security - Part 1: General Model, December 1999.

15. ISO/IEC 15408-2 Information Technology - Security Techniques - Evaluation Criteria for IT Security - Part 2: Security Functional Requirements, December 1999.

16. ISO/IEC 15408-3 Information Technology - Security Techniques - Evaluation Criteria for IT Security - Part 3: Security Assurance Requirements, December 1999.

17. NAS-SR-1000, National Airspace System (NAS) System Requirements Specification, April 2002.

18. National Airspace System Architecture System Engineering Management Plan, version 4.1, 6 February 2003.

19. National Airspace System Architecture Risk Management Plan, version 1.0, 20 March 2003.

20. NIST Special Publication 800-18, Guide for the Development of Security Plans for Information Technology Systems.

21. NSA Information Assurance Technical Framework (IATF), version 3.0, September 30, 2000.

1.2.4 Organization

The main components of a Protection Profile are the Target of Evaluation (TOE) description, Security Environment, Security Objectives, Security Requirements, and Rationale.

Section 2 provides general information about the TOE and its relationship to other FAA systems, serves as an aid to understanding the TOE security requirements, and provides a context for the Protection Profile's evaluation.

Section 3 describes security aspects of the environment in which the TOE will operate. The security environment includes descriptions of: (a) assumptions regarding the intended usage and operational environment, (b) threats relevant to secure operation, and (c) organizational security policies.

Security Objectives, Section 4, reflect the stated intent of the Protection Profile. In particular they pertain to how the TOE will counter identified threats, enforce identified organizational security policies, and uphold assumptions stated in Section 3. Each security objective is categorized as being for the TOE or for the environment.

Security Requirements, Section 5, specifies detailed security requirements. The security requirements are subdivided as follows: (a) functional security requirements - security functions that must be implemented by the system, and (b) security assurance requirements - requirements explaining the actions necessary to verify the integrity of security functions. In addition, requirements are specified for the IT and non-IT environments.

The Rationale, Section 6, presents evidence that the Protection Profile is a complete and cohesive set of security requirements and that a conformant TOE would effectively address stated security needs. The Rationale is organized in two parts. First, a Security Objectives Rationale demonstrates that the stated security objectives counter potential threats, enforce organizational security policies, and adhere to intended usage assumptions. Second, a Security Requirements Rationale demonstrates that the security requirements, both functional and assurance, are traceable to the security objectives and are suitable to meet them. In addition, the appropriateness of the specified Evaluation Assurance Level (EAL) is demonstrated.

1.2.5 Acronyms and Abbreviations

The following acronyms are used in the context of this document as defined below.

AMA	Assurance Maintenance class
AMS	Acquisition Management System (FAA)
CA	Certification Agent
C&A	Certification and accreditation (general usage); certification and authorization (FAA usage)
CC	Common Criteria
CCB	Configuration Control Board
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Implementation and Management Board
CCTL	Common Criteria Testing Lab
CEM	Common Evaluation Methodology
CM	Configuration Management
COTS	Commercial off-the-shelf
CSIRC	Computer Security Incident Response Center
DID	Data Item Description
DOT	Department of Transportation
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GAO	General Accounting Office
IFMS	Invoice and Financial Management Services
IEC	International Electro-technical Commission, Brussels, Belgium
IPT	Integrated Product Team
IS	Information System
ISD	In-service Decision
ISO	Information System Owner
ISO	International Organization for Standardization, Brussels, Belgium
ISSO	Information System Security Officer
IT	Information Technology
LAN	Local Area Network
LOE	Level of Effort
NAS	National Airspace System
NCP	NAS Change Proposal
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NMO	Network Management and Operations
OIG	Office of the Inspector General
O&M	Operations and Maintenance
OMB	Office of Management and Budget
OSP	Organization Security Policy
PP	Protection Profile

SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SIA	Security Impact Analysis
SIR	Screening Information Request
SOF	Strength of Function
SOW	Statement of Work
ST	Security Target
TOE	Target of Evaluation
WAN	Wide Area Network

1.3 ISO/IEC 15408 Conformance

This Protection Profile conforms to the following international standards, as required by FAA Order 1370.82:

- ISO/IEC 15408(12-99), Information Technology – Security Techniques – Criteria for the Evaluation of IT Security, Part 1: General Model.

- ISO/IEC 15408(12-99), Information Technology – Security Techniques – Criteria for the Evaluation of IT Security, Part 2: Security Functional Requirements, extended as indicated in Sections 5.3 and 5.4.

- ISO/IEC 15408(12-99), Information Technology – Security Techniques – Criteria for the Evaluation of IT Security, Part 3: Security Assurance Requirements, augmented as indicated in Section 5.2.

2
Description

This section provides a high-level description of the TOE and its relationship to other FAA systems.

2.1 System Type

The TOE is a low risk application system that will operate within the U.S. National Airspace System (NAS). The NAS is defined as "the common network of U.S. airspace; air navigation facilities, equipment and services; airports or landing areas; aeronautical charts, information and services; rules, regulations and procedures; technical information; and manpower and material. The NAS encompasses everything and everyone providing FAA-regulated flight operations support services to aviators in airspace for which the United States has jurisdiction or responsibility. Included are system components shared jointly with the military. The NAS is an evolving system of technologies, procedures, and people intended to meet the needs of NAS users and service providers. In short, the NAS is a system of systems that executes a safety-critical mission on a 7x24 basis nationwide.

In the FAA environment NAS-SR-1000, the NAS Requirements Specification, is the top-level requirements specification from which all other system requirements specifications are derived. In particular Section 3.8.5 specifies the top-level information systems security requirements to which all NAS systems must comply. NAS-SR-1000 defines three categories of system criticality:

- **Critica**l: Functions or services which, if lost, would prevent the NAS from exercising safe separation and control over aircraft.

- **Essential**: Functions or services which, if lost, would reduce the capability of the NAS to exercise safe separation and control over aircraft.

- **Routine**: Functions or services which, if lost, would not significantly degrade the capability of the NAS to exercise safe separation and control over aircraft.

These definitions can be translated into measures of robustness and resiliency for the key security features of confidentiality, integrity, and availability, as shown in Table 2-1. FIPS PUB 199 defines three levels of system risk: high, moderate, and low. The high risk definition corresponds to a NAS-SR-1000 critical system. The definition for moderate risk corresponds to a NAS-SR-1000 essential system. And, the definition for low risk corresponds to a NAS-SR-1000 routine system.

This PP is for a low risk/routine system.

Table 2-1. Correlation of System Criticality and System Risk

NAS-SR-1000 System Criticality	Security Robustness/Resilience			FIPS PUB 199 System Risk	Security Integrity
	Low	Moderate	High		
Critical		Confidentiality	Availability Integrity	High	EAL 3+
Essential		Confidentiality Integrity	Availability	Moderate	EAL 3+
Routine	Confidentiality Integrity	Availability		Low	EAL 2+

2.2 System Assets

This subsection identifies the NAS assets that require protection.

Table 2-2 summarizes NAS assets by type and sensitivity. The asset categories may be further refined and subdivided in the Security Targets developed in response to this Protection Profile. As shown, there are three main categories of NAS system assets:

- Voice and data
- The hardware, software, and firmware from which the TOE is constructed
- The data and documentation used to operate and maintain the TOE

Table 2-2. NAS Assets and Sensitivities

Information	Security Classification
I. FAA Operational Voice and Data	
1.1 Air to Ground Voice	SBU
1.2 Air to Ground Data	SBU
1.3 Ground to Ground Voice	SBU
1.4 Ground to Ground Data	SBU
1.5 Ground to Air Voice	SBU
1.6 Ground to Air Data	SBU
II. System Hardware, Software, Firmware	
2.1 Cryptographic Keys, other security credentials	SSI
2.2 Cryptographic Equipment	SSI
2.3 Application System (hardware, software, firmware)	FOUO

Information	Security Classification
2.4 LAN/WAN telecommunications infrastructure (hardware, software, firmware)	FOUO/SSI
2.5 System Operation and Management hardware, software, firmware	FOUO/SSI
2.6 Security management hardware, software, firmware	FOUO/SSI
2.7 End-user system hardware, software, firmware	FOUO/SSI
2.8 Interfaces to Military, Law Enforcement, and Other Government Agencies	FOUO/SSI
III. System Operational Data and Documentation[1]	
3.1 Personnel Access Lists and Clearances	SSI
3.2 Operational Security Threats and Alerts	SSI
3.3 Security Incident Reports and Statistics	FOUO/SSI
3.4 Information System Security Plans	FOUO/SSI
3.5 Vulnerability, Threat, and Risk Assessments	FOUO/SSI
3.6 Security Assurance Evidence; Test Plans, Procedures, and Results	FOUO/SSI
3.7 LAN/WAN Telecommunications infrastructure (hardware, software, firmware) configuration information	FOUO/SSI
3.8 Network Management Information	FOUO/SSI
3.9 Security Configuration and Management Information	SSI
3.10 System Design, Operation, and Interface Information	FOUO/SSI
3.11 Logistics Support Data	NR
3.12 Contingency and Disaster Recovery Plans	FOUO/SSI
3.13 Security Architecture and Concept of Operations	FOUO/SSI
3.14 Protection Profiles, Security Targets	FOUO/SSI
3.15 Decommissioning Plans	NR
3.16 Outage Data, Trouble Tickets	SBU

Key: NR - not rated, public information
SBU - sensitive but unclassified
FOUO - for official use only
SSI - security sensitive information

[1] Note: this information may be online, archived, and/or in hardcopy format.

Within the TOE, a variety of user groups will have access to NAS assets for different reasons. As a result, in this document the term "user" includes all of the following categories:

- Contractor network management staff
- Contractor security management staff
- Contractor hardware/software operations and maintenance technicians
- FAA application systems end-users
- FAA security management staff
- FAA hardware/software operations and maintenance technicians
- Trusted partners (airlines, international, etc.)

Access control rights and privileges, which form the foundation of the TOE access control policy, are defined in Table 2-3; no access to assets is allowed other than those explicitly defined or inferred in this table or the Security Targets for the TOE.

Table 2-3. Access Control Rights and Privileges

1.1 Air to Ground Voice	None	None	None	None	None	None	R, CR, CO	R, CR
1.2 Air to Ground Data	None	None	None	None	None	None	R, W, ED, D, CR, CO, F	R, CR
1.3 Ground to Ground Voice	None	None	None	None	None	None	R, CR, CO	R, CR
1.4 Ground to Ground Data	None	None	None	None	None	None	R, W, ED, D, CR, CO, F	R, CR
1.5 Ground to Air Voice	None	None	None	None	None	None	R, CR, CO	R, CR
1.6 Ground to Air Data	None	None	None	None	None	None	R, W, ED, D, CR, CO, F	R, CR
2.1 Cryptographic Keys	None	CO, F, EX, IN	None	None	EX	EX	EX	EX
2.2 Cryptographic Equipment	None	EX	IN	None	EX	EX	None	None

Asset	Contractor Network Mgmt Staff	Contractor Security Mgmt Staff	Contractor O&M Technicians	FAA Network Mgmt Staff	FAA Security Management Staff	FAA O&M Technicians	FAA applications system end-users	Trusted partners
2.3 Application System (hardware, software, firmware)	R, W, ED, D, CR, CO, EX, IN	R, W, ED, D, CR, CO, EX, IN	R, IN, EX	R, IN, EX	R, W, ED, D, CR, CO, F, EX, IN	R, IN, EX	None	None
2.4 LAN/WAN Telecommunications infrastructure (hardware, software, firmware)	R, W, ED, D, CR, CO, EX, IN	R, W, ED, D, CR, CO, EX, IN	R, EX, IN	R, W, ED, D, CR, CO, EX, IN	R, W, ED, D, CR, CO, EX, IN	R, EX, IN	EX	EX
2.5 System Operation and Management hardware, software, firmware	R, W, ED, D, CR, CO, EX, IN	R, W, ED, D, CR, CO, EX, IN	R, EX, IN	R, W, ED, D, CR, CO, EX, IN	R, W, ED, D, CR, CO, EX, IN	R, EX, IN	None	None
2.6 Security management hardware, software, firmware	None	R, W, ED, D, CR, CO, EX, IN	R, EX, IN	None	R, W, ED, D, CR, CO, EX, IN	R, EX, IN	None	None
2.7 End-user System hardware, software, firmware	R, EX, IN	R, EX, IN	R, EX, IN	R, EX, IN	R, EX, IN	R, EX, IN	EX	EX
2.8 Interfaces to Military, Law Enforcement and other Government Agencies	R, EX, IN	R, EX, IN	R, EX, IN	R, EX, IN	R, EX, IN	R, EX, IN	R	None
III. System Operational Documentation and Data								
3.1 Personnel Access Lists and Clearances	R	R	None	R, CR	R, CR	None	None	None
3.2 Security Threats and Alerts	None	R, W, CR, ED, CO, F	None	None	R, W, CR, ED, CO, F	None	None	None
3.3 Security Incident Reports and Statistics	None	R, W, CR, ED, CO, F	None	None	R, W, CR, ED, CO, F	None	None	None

Asset	Contractor Network Mgmt Staff	Contractor Security Mgmt Staff	Contractor O&M Technicians	FAA Network Mgmt Staff	FAA Security Management Staff	FAA O&M Technicians	FAA applications system end-users	Trusted partners
3.4 Information System Security Plan	None	R, W, CR, ED, CO, F	None	None	R, W, CR, ED, CO, F	None	None	None
3.5 Vulnerability, Threat, and Risk Assessments	None	R, W, CR, ED, CO, F	None	None	R, W, CR, ED, CO, F	None	None	None
3.6 Security Assurance Evidence; Test Plans, Procedures, and Results	None	R, W, CR, ED, CO, F	None	None	R, W, CR, ED, CO, F	None	None	None
3.7 LAN/WAN Telecommunications infrastructure (hardware, software, firmware) configuration information	R, W, CR, ED, D, F	R	R	R, W, CR, ED, D, F	R	R	None	None
3.8 System Operation and Management Information	R, W, CR, ED, D, CO, F	R	R	R, W, CR, ED, D, CO, F	R	R	None	None
3.9 Security Configuration and Management Information	None	R, W, ED, D, CR, CO, F	None	None	R, W, ED, D, CR, CO, F	None	None,	None
3.10 System Design, Operation, and Interface Information	R, W, CR, ED, D, F	R	R	R, W, CR, ED, D, F	R	R	None	None
3.11 Logistics Support Data	R, W, ED, CR, D, CO, F	R, W, ED, CR, D, CO, F	R, W, ED, CR, D, CO, F	R, W, ED, CR, D, CO, F	R, W, ED, CR, D, CO, F	R, W, ED, CR, D, CO, F	None	None
3.12 Contingency and Disaster Recovery Plans	R, W, ED, CR, D, CO, F	R, W, ED, CR, D, CO, F	R, W, ED, CR, D, CO, F	R, W, ED, CR, D, CO, F	R, W, ED, CR, D, CO, F	R, W, ED, CR, D, CO, F	None	None

Asset	Contractor Network Mgmt Staff	Contractor Security Mgmt Staff	Contractor O&M Technicians	FAA Network Mgmt Staff	FAA Security Management Staff	FAA O&M Technicians	FAA applications system end-users	Trusted partners
3.13 Security Architecture and Concept of Operations	R, W, ED, CR, D, CO, F	R, W, ED, CR, D, CO, F	R, W, ED, CR, D, CO, F	R, W, ED, CR, D, CO, F	R, W, ED, CR, D, CO, F	R, W, ED, CR, D, CO, F	None	None
3.14 Protection Profiles, Security Targets	R, W, ED, CR, D, CO, F	R, W, ED, CR, D, CO, F	R, W, ED, CR, D, CO, F	R, W, ED, CR, D, CO, F	R, W, ED, CR, D, CO, F	R, W, ED, CR, D, CO, F	None	None
3.15 Decommissioning Plans	R, W, ED, CR, D, CO, F	R, W, ED, CR, D, CO, F	R, W, ED, CR, D, CO, F	R, W, ED, CR, D, CO, F	R, W, ED, CR, D, CO, F	R, W, ED, CR, D, CO, F	None	None
3.16 Outage Data, Trouble Tickets	R, W, ED, CR, D, CO, F	R, W, ED, CR, D, CO, F	R, W, ED, CR, D, CO, F	R, W, ED, CR, D, CO, F	R, W, ED, CR, D, CO, F	R, W, ED, CR, D, CO, F	None	None

Note: Access permissions apply to current as well as archived data.

Key R: read (view data, run canned and ad hoc reports, download reports), hear voice transmissions
W: write (fill in information)
ED: edit (modify existing information)
D: delete (mark a file or record for deletion; do not actually erase it, retain for an audit trail)
CR: create (new record, file, report), initiate voice communication
CO: copy (information to local workstation, backup repository, or archive)
F: forward (send information to another user)
EX: execute (system software/firmware, BITE, etc.)
IN: install or upgrade (COTS hardware or software)
None: no access

2.3 Security Enclaves

The NAS and the compendium of Administrative and Mission Support systems are divided into three security enclaves:

- WAN
- LAN/Facility communications
- Application systems

Each enclave is responsible for boundary protection, the security functions provided within the enclave and the integrity of those functions, and controlling what information enters and exits the enclave. Each enclave is subject to dissimilar threats and vulnerabilities. As a result, different counter measures are deployed at various layers of the protocol stack. Table 2-4 maps the security enclaves to the ISO/OSI reference model.

This TOE belongs to the application system security enclave.

Table 2-4. Delineation of Security Enclaves

ISO/OSI Reference Model	WAN	LAN/Facility Communications	Application Systems
Layer 1 - physical	X	X	
Layer 2 – data link	X	X	
Layer 3 - network	X	X	
Layer 4 - transport		X	
Layer 5 - session			X
Layer 6 - presentation			X
Layer 7 - application			X

3
Security Environment

This section defines the assumptions, threats, and organizational security policies that are applicable to the TOE.

3.1 Assumptions[2]

The statement of the TOE security environment describes the security aspects of the environment in which the TOE is intended to be used and the manner in which it is expected to be employed. The assumptions fall into two main categories:

(1) Information about the intended usage of the TOE, including such aspects as the intended application, potential asset value, and possible limitations of use.

(2) Information about the environment of the TOE, including physical, personnel, and connectivity aspects.

3.1.1 Intended Usage

Intended Application

A-1 Security administration and operations are performed in accordance with the accepted NAS security concept of operations.

A-2 Sufficient safeguards are provided to reduce the risk of a denial-of-service attack to an acceptable level, consistent with specified reliability maintainability and availability (RMA) categories defined for NAS system effectiveness in NAS SR-1000 Section 3.8.

A-3 NAS components rely on an underlying operating system and firmware that are assumed to be installed and operated in a secure manner, i.e. in accordance with the Security Target and guidance documents for the relevant product(s).

A-4 Potential attackers (i.e. threat agents) are assumed to be insiders or outsiders who have a medium to high level of expertise, resources, and motivation.

A-5 NAS systems shall provide hierarchical domains for system access: a) only authorized users shall have access to the information of a particular domain, b) users shall be permitted to access information in domains of equal or lower privilege, c) domains of higher privilege shall be protected from domains of lower privilege, d) shared information shall be capable of being mapped to two or more domains, and e) explicit authorization shall be required for a user to perform any function or access a given view.

[2] Some assumptions may appear as OSPs to the reader; however, if there is no FAA Order to enforce the item, FAA considers it an assumption. Also, please note that some assumptions address the interaction among multiple systems.

A-6 NAS files are assumed to be protected from unauthorized access by the underlying operating system.

Limitations

A-7 NAS Systems may be developed and deployed employing Evolutionary Spiral Process (ESP) methodology over multiple years; hence not all functionality may be deployed at the initial delivery.

A-8 FAA orders, AIS guidelines, and other policies and procedures cited in Section 1.2.3 of this PP limit: connections to the NAS, shared accounts, remote connections to the NAS, use of modems, installation of non-approved software, and procedures for computer equipment disposal.

A-9 Systems must not reduce the overall security posture of the NAS. Countermeasures above and beyond just protecting the system must be considered to prevent the system from introducing additional security risk to the NAS as a whole. Connection to security domains outside the FAA (e.g., ARINC, other states' Civil Aviation Administration) must be limited and controlled because of the potential risks.

A-10 Given the nature of FAA's mission, the majority of NAS Operational data is highly perishable.

A-11 A variety of users will have access to NAS systems and data for different reasons and with a different need-to-know. Accordingly, access control rights and privileges will be limited by type of user, as defined in Table 2-3 of this PP.

3.1.2 Environment of Use

Physical

A-12 Some NAS Systems will be located within controlled access facilities that will prevent unauthorized physical access.

A-13 Some NAS Systems lack adequate physical protection and will require additional physical and technical measures to detect and, if possible, prevent unauthorized physical access.

A-14 NAS Systems critical to security policy enforcement will be physically protected from unauthorized access by potentially hostile outsiders.

A-15 NAS hardware and software critical to security functionality are protected from unauthorized modification by hostile insiders or outsiders.

A-16 Adequate Contingency and Disaster Recovery (C&DR) plans provide countermeasures for natural disasters or deliberate attacks that could result in critical operations being halted and/or NAS services being interrupted.

A-17 NAS backup data repository and archives are located in a secure off-site facility with environmental controls sufficient to ensure data integrity and usability for 2 years. Chain of custody rules for evidence and evidence preservation shall be enforced throughout this time interval.

Personnel

A-18 All authorized administrators and operators of NAS Systems will be adequately trained, enabling them to effectively implement technical and non-technical security policies, including administrative, physical, and procedural security.

A-19 NAS system administrators will coordinate the resolution of security incidents with the CSIRC.

A-20 All authorized administrators and operators of NAS Systems will receive regularly scheduled education and training activities.

A-21 All authorized users are trusted to not act maliciously, nor attempt to circumvent nor by-pass access controls.

A-22 Authorized users will be assigned to manage NAS Systems, including the security of the information it contains.

A-23 Users possess the necessary privileges, based on roles that comply with least-privilege criteria, to access the information they require to perform their assigned duties.

A-24 All authorized NAS users are competent to protect NAS security and the sensitivity of the information transmitted/processed in accordance with applicable FAA Orders.

A-25 A superset of system administrators and managers will oversee the implementation of FAA Policies and Orders relating to the connection of NAS information systems with the Internet. Responsibilities include operational, technical, physical, and critical infrastructure aspects of security, so security protection measures and incident responses can be decided on and carried out. They administer the NAS-wide security controls provided for the benefit of multiple NAS Systems, particularly NAS boundary protections to mitigate risks from connections between the systems within the NAS and systems external to the NAS (e.g., a system operated by a trusted partner).

A-26 A superset of system administrators and managers is responsible for developing system security guidelines, assessing the information security risks to the NAS from connection to security domains external to the FAA, and reporting findings and recommendations to AIS-1. This group has the authority to audit NAS systems and to disable systems network connections that do not comply with these guidelines.

A-27 A superset of system administrators and managers provides a single voice for NAS in the event of a security incident that involves law enforcement and/or national security officials.

Connectivity

A-28 Connection among security domains requires DAA Authorization, based upon information provided in the security Certification and Authorization (C&A) package, specifically the Information System Security Plan (ISSP), prior to establishing that interconnection. If the interconnection is with a system for which another DAA is responsible, then both DAA's must authorize the interconnection. (FAA Order 1370.82, Section 13e[6]).

A-29 FAA Order 1370.83 governs connection to and use of the Internet.

A-30 This PP will be issued as part of an agency procurement. The RFP will include an interface specification for the entire system, including the Application System Security Function component.

3.2 Threats

This subsection identifies potential security threats to the TOE. In particular it:

- Identifies potential security threats to assets by security enclave
- Categorizes the severity of the consequences of each threat
- Qualitatively assesses the likelihood of each threat being instantiated
- Assigns a risk mitigation priority based on the correlation of severity and likelihood

Standard IEC 61508-7 definitions of severity and likelihood are used throughout.

3.2.1 Potential Threats to Assets by Security Enclave

This subsection provides a description of potential threats to assets, against which protection is required. At a high level, potential threats to assets fall into two categories:

1) The accidental or malicious intentional compromise of information confidentiality, integrity, and availability by insiders or outsiders.

2) The accidental or malicious intentional interruptions to operations due to failures of hardware, software, communication links, power supplies, storage media, etc.

Table 3-1 lists potential threats to assets by security enclave. As stated in Assumption A-6, the threat agents are assumed to be insiders or outsiders who have a medium to high level of expertise, resources, and motivation.

Table 3-1. Potential Threats to Assets by Security Enclave

#	Threat	WAN	LAN/ Facility Communications	End-User Applications
A compromise of assets may occur as a result of:				
T1a	An authorized user intentionally or otherwise performs actions the individual is not authorized to perform	X	X	X
T1b	An attacker, whether an insider or outsider, masquerades as an authorized use and attempts to gain access to resources and perform actions that the individual is not authorized to perform	X	X	X
T1c	An attacker (outsider or insider) gains unauthorized access to information or resources by impersonating an authorized user	X	X	X
T1d	An authorized or unauthorized user accidentally or intentionally blocks operational staff from resources	X	X	X
T1e	An unauthorized user gains control of resources	X	X	X
T1f	An authorized or unauthorized user renders resources inoperable	X	X	X
T1g	An unauthorized person attempts to bypass security	X	X	X
T1h	An unauthorized person repeatedly tries to guess user identity and authentication data	X	X	X
T1i	An unauthorized person uses valid identification and authentication data	X	X	X
T1j	An unauthorized person or external IT entity views, modifies, and/or deletes security relevant information that is sent between a remotely located authorized user or administrator	X	X	X
T1k	An authorized or unauthorized user initiates replay attacks	X	X	X
T2	An authorized user accesses information or resources without having permission from the person who owns, or is responsible for, the information or resource.	X	X	X
T3	An authorized or unauthorized user eavesdrops on or otherwise captures data being transferred across a network by performing traffic analysis or using residual information from previous information flows	X	X	
T4	An authorized user or unauthorized outsider consumes global resources in a way that compromises the ability of other authorized users to access or use those resources by circuit jamming (voice or	X	X	X

#	Threat	WAN	LAN/ Facility Communications	End-User Applications
	data), DoS, DDos attacks (voice or data), or theft of service			
T5	An authorized user intentionally or accidentally transmits sensitive information to users who are not cleared to see it.	X	X	X
T6	A user participates in the transfer of information either as originator or recipient and then subsequently denies having done so.		X	X
T7	An authorized user exports information in soft- or hardcopy form, which the recipient subsequently handles in a manner that is inconsistent with its sensitivity designation.		X	X
The integrity and availability of information may be compromised due to:				
T8a	User errors, firmware errors, hardware errors, or transmission errors may compromise the integrity and availability of information	X	X	X
T8b	The unauthorized modification or destruction of information by an attacker may compromise the integrity and availability of information	X	X	X
T8c	Human errors or a failure of software, firmware, hardware or power supplies causes an abrupt interruption to operations, resulting in the loss or corruption of critical data	X	X	X
T8d	Aging of storage media, or improper storage or handling of removable media may compromise the integrity and availability of information	X	X	X
T8e	An authorized user unwittingly introduce a virus into the system and compromise the integrity and availability of information	X	X	X
T8f	An authorized user may introduce unauthorized software into a system and compromise the integrity and availability of information	X	X	X
T8g	An authorized or unauthorized user inserting malicious code or backdoors may compromise the integrity and availability of information	X	X	X
T8h	An unauthorized person reading, modifying, or destroying security critical configuration information may compromise the integrity and availability of information	X	X	X
T8i	A system administrator may fail to perform adequate system backups and compromise the integrity and availability of information	X	X	X

#	Threat	WAN	LAN/ Facility Communications	End-User Applications
T8j	A system administrator may fail to adequately protect storage media and compromise the integrity and availability of information	X	X	X
T8k	Authorized or unauthorized users may accidentally or intentionally delete data and compromise the integrity and availability of information	X	X	X
T8l	Authorized or unauthorized users may insert bogus data and compromise the integrity and availability of information	X	X	X
T8m	Authorized or unauthorized users may accidentally or intentionally modify data	X	X	X
T9	An attacker observes the legitimate use of a resource or service by a user, when the user wishes their use of that resource or service to be kept confidential.	X	X	X
T10	An authorized user may, intentionally or accidentally, observe information stored by a system that the user is not cleared to see.	X	X	X
T11	Security-critical parts of a system may be subject to physical attack which compromises security, including tampering with protection mechanisms.	X	X	X
An authorized insider or unauthorized outsider may accidentally or intentionally cause:				
T12a	Legitimate audit records to be lost or overwritten	X	X	X
T12b	Audit records not to be attributed to time of occurrence	X	X	X
T12c	Audit records not to be attributed to actual source of activity	X	X	X
T12d	Authorized users not to be accountable for their actions because audit records are not reviewed	X	X	X
T12e	Compromises of user or system resources to go undetected for long periods of time	X	X	X
T13	Insiders or outsiders exploit weaknesses in the system architecture, design, implementation, operation, or maintenance that precipitates information security failures.	X	X	X
T14	An authorized insider or unauthorized outsider may cause the improper restart and/or recovery from failure of hardware, software, and/or firmware that causes an information security compromise.	X	X	X
T15	Insiders or outsiders may accidentally or intentionally cause changes in the operational environment that introduces or exacerbates vulnerabilities.	X	X	X
T16	A knowledgeable adversary may	X	X	X

#	Threat	WAN	LAN/ Facility Communications	End-User Applications
	circumvent unexpected limitations or latent defects in countermeasures and mitigation strategies.			
T17	Insiders may accidentally or intentionally define, implement, and enforce access control rights and privileges in a manner that undermines security.	X	X	X
T18	Outsiders initiate natural disasters or acts of war or terrorism that result in critical operations being interrupted or halted.	X	X	X
T19	Compromise of IT assets may occur as a result of actions taken by careless, willfully negligent or hostile administrators or other privileged users; for example: (a) improper operation of hardware, software, and/or firmware, (b) premature hang-up of voice circuit, (c) premature shut-down of PVC or VPN, or (d) careless development and assignment of user roles.	X	X	X
T20	IT assets may be compromised accidentally by insiders as a result of inadequate OPSEC procedures, unfamiliarity with OPSEC procedures, or poorly written OPSEC procedures.	X	X	X

3.2.2 Risk Mitigation Priority

Table 3-2 identifies the severity and likelihood of potential threats to assets so that risk mitigation activities, countermeasures, and resources can be prioritized and applied to the most critical needs.

Table 3-2. Risk-based Analysis of Potential Threats to Assets.

#	Threat	Severity of Consequences	Likelihood of Occurring	Risk Mitigation Priority
A compromise of assets may occur as a result of:				
T1a	An authorized user intentionally or otherwise performs actions the individual is not authorized to perform	marginal to critical	remote	medium
T1b	An attacker, whether an insider or outsider, masquerades as an authorized user and attempts to gain access to resources and perform actions that the individual is not authorized to perform	marginal to critical	occasional	high

#	Threat	Severity of Consequences	Likelihood of Occurring	Risk Mitigation Priority
T1c	An attacker (outsider or insider) gains unauthorized access to information or resources by impersonating an authorized user	marginal to critical	occasional	high
T1d	An authorized or unauthorized user accidentally or intentionally blocks operational staff from system resources	marginal to critical	occasional	high
T1e	An unauthorized user gains control of system resources	marginal to critical	remote	medium
T1f	An authorized or unauthorized user renders system resources inoperable	marginal to critical	remote	medium
T1g	An unauthorized person attempts to bypass security	marginal to critical	frequent	medium to high
T1h	An unauthorized person repeatedly tries to guess user identity and authentication data	marginal to critical	frequent	medium to high
T1i	An unauthorized person uses valid identification and authentication data	Marginal to critical	probable	medium to high
T1j	An unauthorized person or external IT entity views, modifies, and/or deletes security relevant information that is sent between a remotely located authorized user or administrator	marginal to critical	probable	high
T1k	An authorized or unauthorized user initiates replay attacks	marginal to critical	occasional	medium to high
T2	An authorized user access information or resources without having permission from the person who owns, or is responsible for, the information or resource.	marginal to critical	remote	medium
T3	An authorized or unauthorized user eavesdrops on or otherwise captures data being transferred across a network by performing traffic analysis or using residual information from previous information flows	marginal	remote	low
T4	An authorized user or unauthorized	marginal to	remote	high

#	Threat	Severity of Consequences	Likelihood of Occurring	Risk Mitigation Priority
	outsider consumes global resources in a way that compromises the ability of other authorized users to access or use those resources by circuit jamming (voice or data), DoS, DDos attacks (voice or data), or theft of service	catastrophic		
T5	An authorized user intentionally or accidentally transmits sensitive information to users who are not cleared to see it.	marginal to critical	remote	medium
T6	A user participates in the transfer of information either as originator or recipient and then subsequently denies having done so.	marginal	remote	low
T7	An authorized user exports information in soft- or hardcopy form that the recipient subsequently handles in a manner that is inconsistent with its sensitivity designation.	marginal to critical	occasional	high
The integrity and availability of information may be compromised due to:				
T8a	User errors, firmware errors, hardware errors, or transmission errors may compromise the integrity and availability of information	marginal to catastrophic	occasional	high
T8b	Unauthorized modification or destruction of information by an attacker may compromise the integrity and availability of information	marginal to catastrophic	remote	medium
T8c	Human errors or a failure of software, firmware, hardware or power supplies may cause an abrupt interruption to operations, resulting in the loss or corruption of critical data	marginal to catastrophic	remote	medium
T8d	Aging of storage media, or improper storage or handling of removable media by system administrators may compromise the integrity and availability of information	marginal to catastrophic	remote	medium
T8e	An authorized user may unwittingly introduce a virus into the system and compromise the integrity and availability of information	marginal to catastrophic	frequent	high
T8f	An authorized user may introduce unauthorized software into the system and compromise the integrity and availability of information	marginal to catastrophic	frequent	high
T8g	An authorized or unauthorized user may insert malicious code or backdoors and compromise the integrity and availability of information	marginal to catastrophic	occasional	medium

#	Threat	Severity of Consequences	Likelihood of Occurring	Risk Mitigation Priority
T8h	An unauthorized person may read, modify or destroy security critical configuration information	marginal to catastrophic	occasional	medium to high
T8i	A system administrator may fail to perform adequate system backups and compromise the integrity and availability of information	marginal	occasional	medium
T8j	A system administrator may fail to adequately protect storage media and compromise the integrity and availability of information	marginal	occasional	low
T8k	Authorized or unauthorized users accidentally or intentionally delete data	marginal to critical	occasional	medium to high
T8l	Authorized or unauthorized users insert bogus data	marginal to critical	occasional	medium to high
T8m	Authorized or unauthorized users accidentally or intentionally modify data	marginal to critical	occasional	medium to high
T9	An attacker observes the legitimate use of a resource or service by a user, when the user wishes their use of that resource or service to be kept confidential.	marginal to critical	occasional	high
T10	An authorized user may, intentionally or accidentally, observe information stored by a system that the user is not cleared to see.	marginal to marginal	occasional	medium
T11	Security-critical parts of a system may be subject to physical attack, which may compromise security, including tampering with protection mechanisms.	insignificant to catastrophic	improbable	low
An authorized insider or unauthorized outsider may accidentally or intentionally cause:				
T12a	Legitimate audit records to be lost or overwritten	marginal to critical	remote	medium
T12b	Audit records not to be attributed to time of occurrence	marginal to critical	remote	medium
T12c	Audit records not to be attributed to actual source of activity	marginal to critical	remote	medium
T12d	Authorized users not to be accountable for their actions because audit records are not reviewed	marginal to critical	remote	medium

#	Threat	Severity of Consequences	Likelihood of Occurring	Risk Mitigation Priority
T12e	Compromises of user or system resources go undetected for long periods of time	marginal to critical	remote	medium
T13	Insiders or outsiders may exploit weaknesses in the architecture, design, implementation, operation, or maintenance that precipitate information security failures.	marginal to critical	remote	medium
T14	An authorized insider or unauthorized outsider may cause the improper restart and/or recovery from failure of hardware, software, or firmware that causes an information security compromise.	marginal to critical	remote	medium
T15	Insiders or outsiders may accidentally or intentionally cause changes in the operational environment that introduces or exacerbates vulnerabilities.	marginal to critical	remote	low
T16	A knowledgeable adversary may circumvent unexpected limitations or latent defects in countermeasures and mitigation strategies.	marginal to critical	remote	medium
T17	Insiders may accidentally or intentionally define, implement, and enforce access control rights and privileges in a manner that undermines security.	marginal to critical	remote	medium
T18	Outsiders initiate natural disasters or acts of war or terrorism could result in critical operations being interrupted or halted.	marginal to catastrophic	improbable	low
T19	Compromise of IT assets may occur as a result of actions taken by careless, willfully negligent or hostile administrators or other privileged users; for example: (a) improper operation of hardware, software, and/or firmware, (b) premature hang-up of voice circuit, (c) premature shut-down of PVC or VPN, or (d) careless development and assignment of user roles.	marginal to catastrophic	remote	medium
T20	IT assets may be compromised accidentally by insiders as a result of inadequate OPSEC procedures, unfamiliarity with OPSEC procedures, or poorly written OPSEC procedures.	marginal to catastrophic	remote	medium

Definitions (from IEC 61508-7):

Severity:

a. catastrophic - fatalities and/or multiple severe injuries; loss of one or more major systems.
b. critical - single fatality or severe injury; loss of a major system.
c. marginal - minor injuries; severe system damage.
d. insignificant - possible single minor injury; system damage.

Relative Likelihood:

- frequent - likely to occur frequently, 10^{-2}
- probable - will occur several times, 10^{-3}
- occasional - likely to occur several times over the life of a system, 10^{-4}
- remote - likely to occur at some time during the life of a system, 10^{-5}
- improbable - unlikely but possible to occur during the life of a system, 10^{-6}
- incredible - extremely unlikely to occur during the life of a system, 10^{-7}

3.3 Organizational Security Policies

FAA Order 1370.82, *FAA Information Systems Security Program*, establishes policy and assigns organizational and management responsibilities to ensure implementation of the Computer Security Act of 1987; Office of Management and Budget (OMB) Circular A-130 (Transmittal number 4), FY 2001 Defense Authorization Act (P. L. 106-398), Title X, subtitle G, "Government Information Security Reform," Management of Federal Information Resources; Department of Transportation (DOT) Handbook, DOT H 1350.2, Departmental Information Resources Management Manual (DIRMM), OMB *Guidance On Implementing the Government Information Security Reform Act [Security Act]* (OMB 2001), and Presidential Decision Directive 63 (PDD 63).

This order includes FAA policy concerning delegation of authority, policy implementation, and responsibilities of such officials as members of the FAA Management Board, the Assistant Administrator for Information Services and Chief Information Officer (AIO), the Information Systems Security Certifier (ISSC), the Information Systems Security Certification Agent (ISSCA), the Designated Approving Authority (DAA), the Information Systems Security Manager (ISSM), the Information Systems Security Officer (ISSO), and the Contracting Officer (CO) and Contracting Officer Technical Representative (COTR).

Organizational Security Policies (OSPs) are articulated in numerous statements found in various FAA source documents. They may be implemented using procedural mechanisms, technical mechanisms, or both. OSPs cover the four major security objectives:

- Accountability
- Availability
- Confidentiality
- Integrity

The following list represents the FAA OSPs. The OSPs cover a broad range of security specifications that are needed to meet the four major objectives stated above. OSPs are applicable to all three security enclaves. Included in the list are:

- Mechanisms to associate individual entities (human and information systems) with specific actions. They include notions such as identification, authentication and auditing.
- Mechanisms to ensure resources are available when requested and that there are recovery mechanisms in place when a failure occurs.

- Requirements for protection of information from unauthorized access to information in an information system as well as controlled access to IT processing resources.
- Policy guidance concerning general secure installation and operation of IT, such as the need for appropriate documentation, training, and review processes to operate a system securely. This also includes a number of specific policy statements that protect IT resources from being compromised.
- Requirements for protecting information as it is transmitted from one point to another over a potentially unprotected medium.
- Policies that describe the rules for identifying when the IT system, executables, or data have been corrupted.

3.3.1 Accountability

PG-1 The system shall be capable of assigning a unique identifier to each authenticated network user, (e.g., humans, devices, and processes).

PG-2 The system shall be capable of authenticating individual entities (humans and, where appropriate, information systems) identity before allowing any user to perform any actions other than a well-defined set of operations (e.g., reading from a public web site).

PG-3 If passwords are used for authentication, the system shall proactively maintain "strong" password instantiations and shall not allow the use of dictionary words, numerical representations of dates, and other weak, guessable passwords.

PG-4 If passwords are not adequate for authentication, the system shall be capable of strongly authenticating the claimed user identity before allowing any user to perform any actions other than a well-defined set of operations (e.g., reading from a public web site).

PG-5 Passwords shall have a defined lifetime of 3 months and not be reused.

PG-6 The system shall implement strong authentication of end-users and system administrators.

PG-7 The system shall automatically suspend user accounts after a defined number of failed logon attempts.

PG-8 The system shall display the standard FAA "Logon Warning Banner" at logon.

PG-9 The system shall be capable of generating audit records in support of individual accountability and detection.

PG-10 The system shall protect audit log files against deletion and modification of audit log records, even by system administrators.

PG-11 The system shall maintain and protect system audit trails containing security relevant events from unauthorized deletion or modification.

PG-12 The system shall be capable of executing the access control policy defined in Table 2-2 of this PP.

PG-13 The system shall be capable of enabling access authorization management; i.e., the initialization, assignment, and modification of access rights to data objects with respect to: (1) active entity name or group membership, and (2) such constraints as time-of-day and port-of-entry.

PG-14 The system shall be capable of enforcing separation of duties through its role-based ability to restrict users to specific data objects and to specific actions upon those objects.

PG-15 Authorized security administrators and users will be held accountable for security-relevant actions.

PG-16 The system must be implemented and operated in a manner that represents due care and diligence with respect to risks to the FAA. The system must address secure delivery, installation, generation, and start-up of the system.

PG-17 The system must provide a lifecycle support discipline and control in the processes of refining the system during development and maintenance to contribute to the overall quality and security of the system.

PG-18 The system must be used only for authorized purposes.

3.3.2 Availability

PG-19 The system shall be capable of providing resource allocation features having a measure of resistance to resource depletion.

PG-20 The system shall provide secure recovery features providing a measure of survivability in the face of system failures and compromise.

PG-21 The system shall be capable of controlled sharing of resources, such as printer and mass storage, across a network.

3.3.3 Integrity

PG-22 At start-up, the system shall perform a self-check for the presence and correct operating capability of the security function, and shall abort and alarm upon negative findings.

PG-23 The system shall be capable of monitoring file integrity and generating alerts when file integrity is compromised.

PG-24 The system shall be capable of removing or isolating malicious code and data from executable programs and communications traffic.

PG-25 Based on the results of a risk assessment, the system shall provide mechanisms for detecting insecure states of hosts and networks.

PG-26 The processing resources of the system must be physically protected in order to ensure that security objectives are met. These resources will be located within controlled access facilities satisfying FAA standards that mitigate unauthorized physical access.

PG-27 Authorized administrators and authenticated users of the system must be adequately trained, enabling them to: (1) effectively implement organizational security policies with respect to their discretionary actions, and (2) support the need for non-discretionary controls implemented to enforce these policies. This will include provisions for periodic and regularly scheduled education and training activities.

PG-28 The system shall be the object of periodic host- and network-based vulnerability assessments.

PG-29 Following system failure, the system shall recover in a secure state.

PG-30 The system will have documentation describing the security features that are available for authorized users to employ to protect their information.

PG-31 The system will have documentation describing the security configuration parameters that are available to authorized security administrators.

PG-32 Security configurations shall regularly be assessed and updated as appropriate.

PG-33 The system Program Management Office (PMO) shall maintain policy and procedures for handling security incidents.

PG-34 The system shall provide for Configuration Management (CM) of system information security functionality.

PG-35 The system shall undergo periodic ISS-related re-certification as prescribed by FAA policy.

PG-36 The system PMO must establish flaw remediation procedures for tracking and correcting discovered security-related flaws.

PG-37 The system must employ security testing to establish that the security policy enforcement function exhibits the properties necessary to satisfy the functional specifications.

PG-38 The system developer and independent tester must employ penetration tests to discover vulnerabilities that might be introduced in the development or operation of the system.

PG-39 System security must be based on a vulnerability assessment that addresses the vulnerability of the system to misuse or contain incorrect configuration.

PG-40 The system shall automatically force a user logoff after an administrator-defined number of minutes of inactivity and send an alert message to an administrator.

PG-41 The system PMO shall develop and identify policies and procedures for system-wide compliance monitoring.

PG-42 The system shall be capable of centralized security incident reporting.

PG-43 The system administrator shall make use of available information security news-lists, publications, bug fix alerts, CERT advisories, etc., as a recurring set of activities.

PG-44 The system shall implement the defined security policy for inbound and outbound packet transmission using COTS technology such as screening, firewall proxy server functionality, as appropriate.

3.3.4 Confidentiality

PG-45 The system shall protect information system security data and functionality from all unauthorized access.

PG-46 The system shall be capable of performing cryptographic processing, based on the results of a risk assessment, for data encryption, authentication, data integrity, and non-repudiation functionality.

PG-47 The system shall be capable of transmitting and receiving cryptographically processed data at the transport layer and below.

PG-48 Information flow among FAA systems and between a system and other non-FAA systems must be in accordance with established FAA information flow policies.

4
Security Objectives

This section delineates security objectives for the TOE and the operational environment. These objectives are derived from an analysis of the assumptions, threats, and organizational security policies (OSPs) articulated in Section 3.

4.1 Security Objectives for the TOE

Table 4-1 lists the security objectives for the TOE and indicates: (1) to which security enclave they apply, and (2) whether the objective prevents, detects, or corrects security incidents. This PP belongs to the Application System security enclave.

Table 4-1. Security Objectives by Security Enclave.

#	Objective	Type	WAN	LAN/ Facility Communications	End-User Application Systems
O1	The system will enable authorized administrators to effectively manage security functions and will ensure that only authorized administrators are able to access such functionality.	P	x	x	x
O2	The system will record any security relevant events to assist in the detection of potential attacks or mis-configuration of the security features that would leave the system susceptible to attack and to hold users accountable for any actions they perform that are relevant to security.	D	x	x	x
O3	The system will control and limit access to the objects and resources they own or are responsible for, on the basis of individual users or identified groups of users.	P	x	x	x
O4	The system will uniquely identify all users, and will authenticate the claimed identity before granting a user access to assets.	P, D	x	x	x
O5	The system will prevent users from gaining access to and performing operations on resources for which their role is not explicitly authorized.	P	x	x	x
O6	The system will protect the confidentiality of information when it is transmitted, processed, or stored.	P	x	x	x
O7	The system will preserve the integrity and sensitivity of information stored, transmitted, and	P	x	x	x

#	Objective	Type	WAN	LAN/ Facility Communications	End-User Application Systems
	processed. Data exported by the system will have sensitivity labels that are an accurate representation of the corresponding internal sensitivity labels.				
O8	The system will detect loss of system integrity, in particular security functions that may affect information integrity.	D	x	x	x
O9	The system will protect itself against external interference or tampering by untrusted subjects or attempts by untrusted subjects to bypass security functions.	P	x	x	x
O10	The system will generate evidence that can be used to prevent an originator of information from successfully denying ever having sent that information, and evidence that can be used to prevent a recipient of information from successfully denying ever having received that information.	P	x	x	x
O11	The system will control the use of resources by its users and subjects so as to prevent denial of service.	P	x	x	x
O12	The system will return to a known secure state by permitting a user to undo transactions in the case of an incomplete series of transactions.	C	x	x	x
O13	The system must control the consumption of global resources by specified users, including the number of concurrent sessions.	P	x	x	x
O14	The system will not be a vehicle for attacking other FAA systems.	P	x	x	x
O15	The system will not be used to introduce hazardous misleading information (HMI).	P	x	x	x
O16	The system will not be used to decrease the availability of other FAA systems.	P	x	x	x
O17	The security posture of other FAA systems will not be decreased because of a single FAA system.	P	x	x	x
O18	External domains not under FAA control are considered potentially hostile entities. Systems connected to such external domains must analyze and attempt to counter hostile actions originating from these domains.	P, D, C	x	x	x

Key: P - prevent
D - detect
C - correct

4.2 Security Objectives for the Operational Environment

Table 4-2 lists the security objectives for the operational environment and whether the objective prevents, detects, or corrects security incidents.

Table 4-2. Operational Environment Security Objectives.

#	Objective	Type
O19	System administrators must ensure that audit facilities are used and managed effectively. In particular appropriate action must be taken to ensure continued audit logging, by regular archiving of logs before audit trail exhaustion to ensure sufficient free space and that audit logs are protected from unauthorized modification and deletion.	P, D, C
O20	System administrators must ensure that the authentication data for each user account is held securely and not disclosed to persons not authorized to use that account.	P
O21	System administrators must ensure that no connections are provided to outside systems or users that would undermine IT security.	P
O22	System administrators must ensure that the system is delivered, installed, managed, operated, and maintained in a secure manner.	P
O23	System administrators must ensure that those parts of the system that are critical to security policy enforcement are protected from physical attack that might compromise IT security.	P
O24	System administrators must ensure that procedures and/or mechanisms are in place to ensure that, after system failure or other discontinuity, recovery without compromise of IT security is obtained.	P
O25	System administrators must ensure that adequate environmental controls and monitoring are in place at the primary and off-site facilities to prevent system degradation or outage due to environmental disruption (power disruption, fire, flood, dust, heat, humidity, vibration, etc.).	P, D, C

Key: P - prevent
D - detect
C - correct

5
Requirements

This section provides detailed security requirements, in separate subsections, for the TOE (5.1), the IT environment (5.3), and the non-IT environment (5.4), including strength of function (SOF) requirements for the TOE security functions realized by probabilistic or permutational mechanisms. The security assurance requirements stated in subsection 5.2 are applicable to the TOE (5.1), the IT environment (5.3) and the non-IT environment (5.4).

5.1 Security Functional Requirements (SFRs)

In the FAA environment NAS-SR-1000, the National Airspace System (NAS) Requirements Specification, is the top-level requirements specification from which all other system requirements specifications are derived. In particular Section 3.8.5 specifies the top-level information systems security requirements to which all NAS systems must comply. (See Table 5-1.) Each of these 10 requirements constitute a functional package:

- Level of security functionality and security integrity
- Security training
- Integrity
- Availability
- Access Control
- Security Audit
- Confidentiality
- Identification and Authentication
- Recovery
- Security Management

Low-level requirements, from the CC components, were derived for each functional package and are stated in subsections 5.1.1 through 5.1.10 below. Each functional package is distinct and self-contained; the complete functionality specified therein shall be provided.

5.1.1 Level of Security Functionality and Security Integrity (3.8.5.A)

This statement in NAS-SR-1000 is a high-level global requirement. All the SFRs and SARs stated below contribute to its fulfillment.

5.1.2 Security Training (3.8.5.B)

Training is an operational security, not an information security requirement. As such, training is not something that can be specified in an IT security requirements specification. The SARs associated with this high-level requirement ensure that the necessary documentation is developed to support the training. SARs are discussed in subsection 5.2 below.

Table 5-1. Enhanced NAS-SR-1000 Information Security Requirements

NAS-SR-1000 Requirement
3.8.5.A All NAS systems shall provide the required level of security functionality and security integrity based upon vulnerability, threat, and risk analyses.
3.8.5.B All NAS systems shall provide the required level of security training based upon the vulnerability, threat, and risk analyses.
3.8.5.C All NAS systems shall be protected from threats to compromise integrity.
3.8.5.D All NAS systems shall be protected from threats to compromise availability.
3.8.5.E All NAS systems shall provide access control.
3.8.5.F All NAS systems shall provide an audit capability sufficient to monitor attempted and successful system intrusions.
3.8.5.G All NAS systems shall provide for information confidentiality based upon the result of a security assessment.
3.8.5.H NAS systems shall implement identification and authentication at a level based upon a security assessment, and non-repudiation when appropriate.
3.8.5.I All NAS systems shall provide recovery measures from security incidents.
3.8.5.J All NAS systems shall provide the capability to centrally manage security functions.

5.1.3 Integrity (3.8.5.C)

The following SFRs shall be implemented to construct the integrity functional package.

Basic Data Authentication

FDP_DAU.1.1+1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of user data.

FDP_DAU.1.1+2 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of security management data.

FDP_DAU.1.1+3 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of system management data.

FDP_DAU.1.2+1 The TSF shall provide authorized end users with the ability to verify evidence of the validity of the indicated information.

FDP_DAU.1.2+2 The TSF shall provide authorized security management staff with the ability to verify evidence of the validity of the indicated information.

FDP_DAU.1.2+3 The TSF shall provide authorized system administrators with the ability to verify evidence of the validity of the indicated information.

Basic Internal Transfer Protection

FDP_ITT.1.1+1 The TSF shall enforce the access control SFP to prevent disclosure of user data when it is transmitted between physically-separated parts of the TOE.

FDP_ITT.1.1+2 The TSF shall enforce the access control SFP to prevent modification of user data when it is transmitted between physically-separated parts of the TOE.

FDP_ITT.1.1+3 The TSF shall enforce the access control SFP to prevent loss of use of user data when it is transmitted between physically-separated parts of the TOE.

FDP_ITT.1.1+4 The TSF shall enforce the information flow control policy to prevent disclosure of user data when it is transmitted between physically-separated parts of the TOE.

FDP_ITT.1.1+5 The TSF shall enforce the information flow control policy to prevent modification of user data when it is transmitted between physically-separated parts of the TOE.

FDP_ITT.1.1+6 The TSF shall enforce the information flow control policy to prevent loss of use of user data when it is transmitted between physically-separated parts of the TOE.

Basic Rollback

FDP_ROL.1.1+1 The TSF shall enforce access control policies to permit the rollback of the:

(a) create operations
(b) modify operations
(c) delete operations
(d) merge operations
(e) insert operations

on the:

(a) user data
(b) security management data
(c) system management data

FDP_ROL.1.1+2 The TSF shall enforce information flow control policies to permit the rollback of the:

(a) create operations
(b) modify operations
(c) delete operations
(d) merge operations
(e) insert operations

on the:

(a) user data
(b) security management data
(c) system management data

FDP_ROL.1.2 The TSF shall permit operations to be rolled back within the previous three transactions.

Stored Data Integrity Monitoring and Action

FDP_SDI.2.1 The TSF shall monitor user data stored within the TSC for integrity errors on all objects, based on the following attributes: checksums, cyclical redundancy checks (CRCs), or hash functions.

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall generate an alarm and notify the system administrator.

Abstract Machine Testing

FPT_AMT.1.1+1 The TSF shall run a suite of tests during initial start-up to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

FPT_AMT.1.1+2 The TSF shall run a suite of tests periodically during normal operations to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

FPT_AMT.1.1+3 The TSF shall run a suite of tests at the request of an authorized user to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

Failure with Preservation of Secure State

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: all system failure modes.

Notification of Physical Attack

FPT_PHP.2.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.2.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_PHP.2.3 For all system components located in FAA or contractor spaces, the TSF shall monitor the devices and elements and notify the system administrator when physical tampering with the TSF's devices or elements has occurred.

Resistance to Physical Attack

FPT_PHP.3.1 The TSF shall resist physical tampering with cables, connectors, interfaces, configuration settings, and operational parameters to all system components by responding automatically such that the TSP is not violated.

Replay Detection

FPT_RPL.1.1 The TSF shall detect replay for the following entities:
(a) user data transmitted,
(b) user data received,

(c) security management data transmitted,
(d) security management data received,
(e) system management data transmitted,
(f) system management data received.

FPT_RPL.1.2+1 The TSF shall perform alarm generation when replay is detected.

FPT_RPL.1.2+2 The TSF shall perform system administrator notification when replay is detected.

Inter-TSF Data Consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret TSF data when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use the same interpretation rules when interpreting the TSF data from another trusted IT product.

Internal TSF Consistency

FPT_TRC.1.1 The TSF shall ensure that TSF data is consistent when replicated between parts of the TOE.

FPT_TRC.1.2 When parts of the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection before processing any requests for: authentication or enforcement of access control or information flow control policies.

TSF Testing

FPT_TST.1.1+1 The TSF shall run a suite of self-tests during initial start-up to demonstrate the correct operation of the TSF.

FPT_TST.1.1+2 The TSF shall run a suite of self-tests periodically during normal operations to demonstrate the correct operation of the TSF.

FPT_TST.1.1+3 The TSF shall run a suite of self-tests at the request of an authorized user to demonstrate the correct operation of the TSF.

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of TSF data.

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

5.1.4 Availability (3.8.5.D)

The following SFRs shall be implemented to construct the availability functional package.

Degraded Fault Tolerance

FRU_FLT.1.1 The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: all system failure modes.

Limited Priority of Service

FRU_PRS.1.1 The TSF shall assign a priority to each subject in the TSF.

FRU_PRS.1.2 The TSF shall ensure that each access to all shareable resources shall be mediated on the basis of the subject's assigned priority.

Maximum Quotas

FRU_RSA.1.1+1 The TSF shall enforce maximum quotas of the following resources: all controlled system resources that individual users can use simultaneously.

FRU_RSA.1.1+2 The TSF shall enforce maximum quotas of the following resources: all controlled system resources that system administrators can use simultaneously.

FRU_RSA.1.1+3 The TSF shall enforce maximum quotas of the following resources: all controlled system resources that security management staff can use simultaneously.

FRU_RSA.1.1+4 The TSF shall enforce maximum quotas of the following resources: all controlled system resources that individual users can use over a specified period of time.

FRU_RSA.1.1+5 The TSF shall enforce maximum quotas of the following resources: all controlled system resources that system administrators can use over a specified period of time.

FRU_RSA.1.1+6 The TSF shall enforce maximum quotas of the following resources: all controlled system resources that security management staff can use over a specified period of time.

5.1.5 Access Control (3.8.5.E)

The following SFRs shall be implemented to construct the access control functional package, in accordance with the access control rights and privileges defined in Tables 2-1 and 2-2 of this PP.

Complete Access Control

FDP_ACC.2.1 The TSF shall enforce the access control policy: on all users and processes acting on their behalf, and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

Security Attribute Based Access Control

FDP_ACF.1.1 The TSF shall enforce the access control policy to objects based on: the explicit rights and privileges of users and subjects.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: explicit access rights and privileges.

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: inferred access rights and privileges.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the fact that the access is neither explicitly authorized nor inferred.

Export of User Data Without Security Attributes

FDP_ETC.1.1+1 The TSF shall enforce the access control policy when exporting user data, controlled under the SFP outside of the TSC.

FDP_ETC.1.1+2 The TSF shall enforce the information flow control policy when exporting user data, controlled under the SFP outside of the TSC.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.

Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the information flow control policy on: all subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the policy.

Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the information flow control policy based on the following types of subject and information security attributes: the security attributes defined for FIA_ATD.1.1.

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: the subject has explicit rights and privileges to perform the operation.

FDP_IFF.1.3 The TSF shall enforce the: separation of information flows between the three major security domains:
(a) end user
(b) security management
(c) system management.

Application note: The end-user security domain may be sub-divided into sub-domains.

FDP_IFF.1.4 The TSF shall provide the following: the ability for authorized security management roles to dynamically update or modify the information flow control policy.

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: the flow is explicitly authorized or inferred.

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: the flow is neither explicitly permitted nor inferred.

No Illicit Information Flows

FDP_IFF.5.1 The TSF shall ensure that no illicit information flows exist to circumvent the information flow control policy.

Import of User Data Without Security Attributes

FDP_ITC.1.1+1 The TSF shall enforce the access control policy when importing user data, controlled under the SFP, from outside the TSC.

FDP_ITC.1.1+2 The TSF shall enforce the information flow control policy when importing user data, controlled under the SFP, from outside the TSC.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: the data shall be scanned for viruses, worms, and other malicious code.

TSF Domain Separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Application note: There are three security domains: (a) end-user, (b) security management, and (c) system management. The end-user security domain may be sub-divided into sub-domains.

5.1.6 Security Audit (3.8.5.F)

The following SFRs shall be implemented to construct the security audit functional package.

Security Alarms

FAU_ARP.1.1 The TSF shall take the following actions: (a) audible alarm generation, (b) visible alarm generation, and (c) automatic notification of system administrator upon detection of a potential security violation.

Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

(a) Start-up and shutdown of the audit function;
(b) All auditable events for the minimal level of audit.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

(a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
(b) For each audit event type, based on the auditable event definitions of the functional components included in the

PP/ST: identity of the objects involved or effected, and the corrective action taken

User Identity Association

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Profile-based Anomaly Detection

FAU_SAA.2.1 The TSF shall be able to maintain profiles of system usage, where an individual profile represents the historical patterns of usage performed by the members of the distinct user groups defined in the access control policy.

FAU_SAA.2.2 The TSF shall be able to maintain a suspicion rating associated with each user whose activity is recorded in a profile, where the suspicion rating represents the degree to which the user's current activity is found inconsistent with the established patterns of usage represented in the profile.

FAU_SAA.2.3 The TSF shall be able to indicate an imminent violation of the TSP when a user's suspicion rating exceeds the following threshold conditions: more than one violation or warning per hour.

Complex Attack Heuristics

FAU_SAA.4.1 The TSF shall be able to maintain an internal representation of the following event sequences of known intrusion scenarios: system events, individually or in combination, that indicate a precursor to, potential, imminent, or actual penetration scenario, and the following signature events: any unauthorized event that may indicate a potential violation of the TSP.

FAU_SAA.4.2 The TSF shall be able to compare the signature events and event sequences against the record of system activity discernible from an examination of: audit information generated by the system and/or security mechanisms.

FAU_SAA.4.3 The TSF shall be able to indicate an imminent violation of the TSP when system activity is found to match a signature event or event sequence that indicates a potential violation of the TSP.

Audit Review

FAU_SAR.1.1 The TSF shall provide authorized users with the capability to read audit information appropriate for their user group from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Restricted Audit Review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

Selectable Audit Review

FAU_SAR.3.1+1 The TSF shall provide the ability to perform searches of audit data based on event type, date, time, subject identity, and/or object identity.

FAU_SAR.3.1+2 The TSF shall provide the ability to perform ordering of audit data based on event type, date, time, subject identity, and/or object identity.

Selective Audit

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:
(a) object identity
(b) user identity
(c) subject identity
(d) host identity
(e) event type

Guarantees of Audit Data Availability

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.2.2+1 The TSF shall be able to prevent modifications to the audit records.

FAU_STG.2.2+2 The TSF shall be able to detect modifications to the audit records.

FAU_STG.2.3+1 The TSF shall ensure that all audit records will be maintained when the following conditions occur: audit storage exhaustion.

FAU_STG.2.3+2 The TSF shall ensure that all audit records will be maintained when the following conditions occur: failure.

FAU_STG.2.3+3 The TSF shall ensure that all audit records will be maintained when the following conditions occur: attack.

Prevention of Audit Data Loss

FAU_STG.4.1 The TSF shall prevent auditable events, except those taken by the authorized user with special rights and: generate audible and visible alarms, if the audit trail is full.

Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

5.1.7 Confidentiality (3.8.5.G)

The following SFRs shall be implemented to construct the confidentiality functional package.

Full Residual Information Protection

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon de-allocation of the resource from all objects.

Anonymity

FPR_ANO.1.1 The TSF shall ensure that all internal or external end-users and/or subjects acting on their behalf are unable to determine the real user name bound to any system resource.

5.1.8 Identification and Authentication (3.8.5.H)

The following SFRs shall be implemented to construct the Identification and Authentication functional package.

Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when 3 unsuccessful authentication attempts occur related to user identification and/or user authentication.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall:
(a) Generate an alarm
(b) Notify the system administrator
(c) Block the user from further activity.

User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:
(a) User identity
(b) Aliases
(c) Password and other security credentials
(d) User group or role to which the user belongs
(e) Security domains to which the user has access
(f) Security domains to which the user does not have access
(g) Explicit access control rights and privileges
(h) Inferred access control rights and privileges
(i) Subjects authorized to act on the user's behalf

Verification of Secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet the requirements of FIPS 140-2 level 2 or higher.

Generation of Secrets

FIA_SOS.2.1 The TSF shall provide a mechanism to generate secrets that meet the requirements of FIPS 140-2 level 2 or higher.

FIA_SOS.2.2 The TSF shall be able to enforce the use of TSF generated secrets for all applicable TOE security functions.

User Authentication Before Any Action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Unforgeable Authentication

FIA_UAU.3.1+1 The TSF shall detect use of authentication data that has been forged by any user of the TSF.

FIA_UAU.3.1+2 The TSF shall prevent use of authentication data that has been forged by any user of the TSF.

FIA_UAU.3.2+1 The TSF shall detect use of authentication data that has been copied from any other user of the TSF.

FIA_UAU.3.2+2 The TSF shall prevent use of authentication data that has been copied from any other user of the TSF.

Re-authenticating

FIA_UAU.6.1 The TSF shall re-authenticate the user under these conditions:

(a) A specified time has elapsed since they were authenticated.
(b) The system experienced an anomaly or partial failure.
(c) The user is active during an unusual time frame for their user group.
(d) The user session has been inactive for a specified time.

Protected Authentication Feedback

FIA_UAU.7.1 The TSF shall provide only a “working message” to the user while the authentication is in progress.

User Identification Before Any Action

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

User-subject Binding

FIA_USB.1.1 The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user.

5.1.9 Recovery (3.8.5.I)

The following SFRs shall be implemented to construct the Recovery functional package.

Destination Data Exchange Recovery

FDP_UIT.3.1+1 The TSF shall enforce the access control policy to be able to recover from system errors without any help from the source trusted IT product.

FDP_UIT.3.1+2 The TSF shall enforce the information flow control policy to be able to recover from system errors without any help from the source trusted IT product.

Automated Recovery Without Undue Loss

FPT_RCV.3.1 When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.

FPT_RCV.3.2 For all system failures the TSF shall ensure the return of the TOE to a secure state using automated procedures.

FPT_RCV.3.3 The functions provided by the TSF to recover from failure or service discontinuity shall ensure that the secure initial state is restored without exceeding any loss of TSF data or objects within the TSC.

FPT_RCV.3.4 The TSF shall provide the capability to determine the objects that were or were not capable of being recovered.

Function Recovery

FPT_RCV.4.1 The TSF shall ensure that all security functions have the property that the security function either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

5.1.10 Security Management (3.8.5.J)

The following SFRs shall be implemented to construct the Security Management functional package.

Management of Security Functions Behavior

FMT_MOF.1.1+1 The TSF shall restrict the ability to determine the behavior of the functions performed by security mechanisms to authorized security management roles.

FMT_MOF.1.1+2 The TSF shall restrict the ability to disable the functions performed by security mechanisms to authorized security management roles.

FMT_MOF.1.1+3 The TSF shall restrict the ability to enable the functions performed by security mechanisms to authorized security management roles.

FMT_MOF.1.1+4 The TSF shall restrict the ability to modify the behavior of the functions performed by security mechanisms to authorized security management roles.

Management of Security Attributes

FMT_MSA.1.1+1 The TSF shall enforce the access control policy to restrict the ability to change default security attributes to authorized security management roles.

FMT_MSA.1.1+2 The TSF shall enforce the access control policy to restrict the ability to query security attributes to authorized security management roles.

FMT_MSA.1.1+3 The TSF shall enforce the access control policy to restrict the ability to modify security attributes to authorized security management roles.

FMT_MSA.1.1+4 The TSF shall enforce the access control policy to restrict the ability to delete security attributes to authorized security management roles.

FMT_MSA.1.1+5 The TSF shall enforce the access control policy to restrict the ability to view security attributes to authorized security management roles.

FMT_MSA.1.1+6 The TSF shall enforce the information flow control policy to restrict the ability to change default security attributes to authorized security management roles.

FMT_MSA.1.1+7 The TSF shall enforce the information flow control policy to restrict the ability to query security attributes to authorized security management roles.

FMT_MSA.1.1+8 The TSF shall enforce the information flow control policy to restrict the ability to modify security attributes to authorized security management roles.

FMT_MSA.1.1+9 The TSF shall enforce the information flow control policy to restrict the ability to delete security attributes to authorized security management roles.

FMT_MSA.1.1+10 The TSF shall enforce the information flow control policy to restrict the ability to view security attributes to authorized security management roles.

Secure Security Attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

Static Attribute Initialization

FMT_MSA.3.1+1 The TSF shall enforce the access control policy to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.1+2 The TSF shall enforce the information flow control policy to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the authorized security management roles to specify alternative initial values to override the default values when an object or information is created.

Management of TSF Data

FMT_MTD.1.1+1 The TSF shall restrict the ability to change the default values of security management data to authorized security management roles.

FMT_MTD.1.1+2 The TSF shall restrict the ability to query the values of security management data to authorized security management roles.

FMT_MTD.1.1+3 The TSF shall restrict the ability to modify the values of security management data to authorized security management roles.

FMT_MTD.1.1+4 The TSF shall restrict the ability to delete the values of security management data to authorized security management roles.

FMT_MTD.1.1+5 The TSF shall restrict the ability to clear the values of security management data to authorized security management roles.

FMT_MTD.1.1+6 The TSF shall restrict the ability to view the values of security management data to authorized security management roles.

Management of Limits on TSF Data

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for security management data to authorized security management roles.

FMT_MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: prevent any further actions until the TSF data returns to normal limits.

Secure TSF Data

FMT_MTD.3.1 The TSF shall ensure that only secure values are accepted for TSF data.

Revocation

FMT_REV.1.1+1 The TSF shall restrict the ability to revoke security attributes associated with the users within the TSC to authorized security management roles.

FMT_REV.1.1+2 The TSF shall restrict the ability to revoke security attributes associated with the subjects within the TSC to authorized security management roles.

FMT_REV.1.1+3 The TSF shall restrict the ability to revoke security attributes associated with the objects within the TSC to authorized security management roles.

FMT_REV.1.2 The TSF shall enforce the rules:

(a) security attributes shall be revoked immediately upon expiration.

(b) Security attributes shall be revoked immediately when a subject or object is no longer part of the system configuration.

Time-limited Authorization

FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for security attributes to authorized security management roles.

FMT_SAE.1.2 For each of these security attributes, the TSF shall be able to revoke the security attributes after the expiration time for the indicated security attribute has passed.

Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles: security management roles.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Limitation on Scope of Selectable Attributes

FTA_LSA.1.1 The TSF shall restrict the scope of the session security attributes [assignment: session security attributes] based on user security attributes.

Basic Limitation on Multiple Concurrent Sessions

FTA_MCS.1.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.

FTA_MCS.1.2 The TSF shall enforce, be default, a limit of 3 sessions per user.

TSF –initiated Session Locking

FTA_SSL.1.1 The TSF shall lock an interactive session after 10 minutes of user inactivity by:

(a) clearing or overwriting display devices, making the current contents unreadable;

(b) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: user re-authentication and re-identification.

TSF_Initiated Termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after 15 minutes of user inactivity.

Default TOE Access Banners

FTA_TAB.1.1	Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

TOE Session Establishment

FTA_TSE.1.1	The TSF shall be able to deny session establishment based on user security attributes.

5.2 Security Assurance Requirements (SARs)

The SARs defined in this subsection are applicable to subsections 5.1, 5.3, and 5.4 of this PP. The development contractor shall perform all of the developer action elements for these SARs. All of the content and presentation of evidence elements shall be produced by the development contractor. All of the evaluator action elements for these SARs shall be performed by the CCTL in accordance with the Common Evaluation Methodology (CEM) and Common Criteria Evaluation and Validation Scheme (CCEVS). These action elements shall be performed and the evidence shall be produced to ensure that the stated Evaluation Assurance Level (EAL 2+) is achieved.

Table 5-2 defines the SARs and EAL for low, moderate, and high risk systems. This PP is for a low risk system; hence the third column is applicable. Subsections 5.2.1 through 5.2.8 below specify the SARs for eight security assurance classes:

- Configuration Management (ACM)
- Delivery and Operations (ADO)
- Development (ADV)
- Guidance Documents (AGD)
- Lifecycle Support (ALC)
- Tests (ATE)
- Vulnerability Assessment (AVA)
- Maintenance of Assurance (AMA)

Note that the security assurance requirements extend into the operations and maintenance (O&M) phase.

5.2.1 Configuration Management (ACM)

The followings SARs shall be performed for the ACM class to ensure that EAL 2+ is achieved, per Table 5-2.

ACM_CAP.3 Authorization Controls

Developer action elements:

ACM_CAP.3.1D	The developer shall provide a reference for the TOE.
ACM_CAP.3.2D	The developer shall use a CM system.
ACM_CAP.3.3D	The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.3.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.3.2C The TOE shall be labeled with its reference.

ACM_CAP.3.3C The CM documentation shall include a configuration list and a CM plan.

ACM_CAP.3.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.3.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.3.6C The CM system shall uniquely identify all configuration items.

ACM_CAP.3.7C The CM plan shall describe how the CM system is used.

ACM_CAP.3.8C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.3.9C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.3.10C The CM system shall provide measures such that only authorized changes are made to the configuration items.

Evaluator action elements:

ACM_CAP.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2 Delivery and Operations (ADO)

The followings SARs shall be performed for the ADO class to ensure that EAL 2+ is achieved, per Table 5-2.

ADO_DEL.1 Delivery Procedures

Developer action elements:

ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Evaluator action elements:

ADO_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1 Installation, generation, and start-up procedures

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action elements:

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3 Development (ADV)

The followings SARs shall be performed for the ADV class to ensure that EAL 2+ is achieved, per Table 5-2.

ADV_FSP.1 Informal functional specification

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

Evaluator action elements:

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

ADV_HLD.1 Descriptive High-level Design

Developer action elements:

ADV_HLD.1.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.1.1C The presentation of the high-level design shall be informal.

ADV_HLD.1.2C The high-level design shall be internally consistent.

ADV_HLD.1.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.1.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

Evaluator action elements:

ADV_HLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.1.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Guidance Documents (AGD)

The followings SARs shall be performed for the AGD class to ensure that EAL 2+ is achieved, per Table 5-2.

AGD_ADM.1 Administrator Guidance

Developer action elements:

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_USR.1 User guidance

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.5 Tests (ATE)

The followings SARs shall be performed for the ATE class to ensure that EAL 2+ is achieved, per Table 5-2.

ATE_COV.1 Evidence of coverage

Developer action elements:

ATE_COV.1.1D The developer shall provide evidence of test coverage.

Content and presentation of evidence elements:

ATE_COV.1.1C The evidence of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

Evaluator action elements:

ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 Functional testing

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2 Independent testing - sample

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.2.6 **Vulnerability Assessment (AVA)**

The followings SARs shall be performed for the AVA class to ensure that EAL 2+ is achieved, per Table 5-2.

AVA_SOF.1 Strength of TOE security function evaluation

Developer action elements:

AVA_SOF.1.1D The developer shall perform a strength of TOE security functional analysis for each mechanism identified in the ST as having a strength of TOE function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action elements:

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

AVA_VLA.1 Developer vulnerability analysis

Developer action elements:

AVA_VLA.1.1D The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2D The developer shall document the disposition of obvious vulnerabilities.

Content and presentation of evidence elements:

AVA_VLA.1.1C The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

AVA_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

5.2.7 Maintenance of Assurance (AMA)

The followings SARs shall be performed for the AVA class to ensure that EAL 2+ is maintained during the operations and maintenance phase and between security C&A cycles, per Table 5-2.

AMA_AMP.1 Assurance maintenance plan

Developer action elements:

AMA_AMP.1.1D The developer shall provide an AM plan.

Content and presentation of evidence elements:

AMA_AMP.1.1C The AM plan shall contain or reference a brief description of the TOE, including the security functionality it provides.

AMA_AMP.1.2C The AM plan shall identify the certified version of the TOE, and shall reference the evaluation results.

AMA_AMP.1.3C The AM plan shall reference the TOE component categorization report for the certified version of the TOE.

AMA_AMP.1.4C The AM plan shall define the scope of changes to the TOE that are covered by the plan.

AMA_AMP.1.5C The AM plan shall describe the TOE life-cycle, and shall identify the current plans for any new releases of the TOE, together with a brief description of any planned changes that are likely to have a significant security impact.

AMA_AMP.1.6C The AM plan shall describe the assurance maintenance cycle, stating and justifying the planned schedule of AM audits and the target date of the next re-evaluation of the TOE.

AMA_AMP.1.7C The AM plan shall identify the individual(s) who will assume the role of developer security analyst for the TOE.

AMA_AMP.1.8C The AM plan shall describe how the developer security analyst role will ensure that the procedures documented or referenced in the AM Plan are followed.

AMA_AMP.1.9C The AM plan shall describe how the developer security analyst role will ensure that all developer actions involved in the analysis of the security impact of changes affecting the TOE are performed correctly.

AMA_AMP.1.10C The AM plan shall justify why the identified developer security analyst(s) have sufficient familiarity with the security target, functional specification and (where appropriate) high-level design of the TOE, and with the evaluation results and all applicable assurance requirements for the certified version of the TOE.

AMA_AMP.1.11C The AM plan shall describe or reference the procedures to be applied to maintain the assurance in the TOE, which as a minimum shall include the procedures for configuration management, maintenance of assurance evidence, performance of the analysis of the security impact of changes affecting the TOE, and flaw remediation.

Evaluator action elements:

AMA_AMP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AMA_AMP.1.2E The evaluator shall confirm that the proposed schedules for AM audits and re-evaluation of the TOE are acceptable and consistent with proposed changes to the TOE.

AMA_CAT.1 TOE component categorization report

Developer action elements:

AMA_CAT.1.1D The developer shall provide a TOE component categorization report for the certified version of the TOE.

Content and presentation of evidence elements:

AMA_CAT.1.1C The TOE component categorization report shall categorize each component of the TOE, identifiable in each TSF representation from the most abstract to the least abstract, according to its relevance to security; as a minimum, TOE components must be categorized as one of TSP-enforcing or non-TSP-enforcing.

AMA_CAT.1.2C The TOE component categorization report shall describe the categorization scheme used, so that it can be determined how to categorize new components introduced into the TOE, and also when to re-categorize existing TOE components following changes to the TOE or its security target.

AMA_CAT.1.3C The TOE component categorization report shall identify any tools used in the development environment that, if modified, will have an impact on the assurance that the TOE satisfies its security target.

Evaluator action elements:

AMA_CAT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AMA_CAT.1.2E The evaluator shall confirm that the categorization of TOE components and tools, and the categorization scheme used, are appropriate and consistent with the evaluation results or the certified version.

AMA_EVD.1 Evidence of maintenance process

Developer action elements:

AMA_EVD.1.1D The developer security analyst shall provide AM documentation for the current version of the TOE.

Content and presentation of evidence elements:

AMA_EVD.1.1C The AM documentation shall include a configuration list and a list of identified vulnerabilities in the TOE.

AMA_EVD.1.2C The configuration list shall describe the configuration items that comprise the current version of the TOE.

AMA_EVD.1.3C The AM documentation shall provide evidence that the procedures documented or referenced in the AM plan are being followed.

AMA_EVD.1.4C The list of identified vulnerabilities in the current version of the TOE shall show, for each vulnerability, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

AMA_EVD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AMA_EVD.1.2E The evaluator shall confirm that the procedures documented or referenced in the AM plan are being followed.

AMA_EVD.1.3E The evaluator shall confirm that the security impact analysis for the current version of the TOE is consistent with the configuration list.

AMA_EVD.1.4E The evaluator shall confirm that all changes documented in the security impact analysis for the current version of the TOE are within the scope of changes covered by the AM plan.

AMA_EVD.1.5E The evaluator shall confirm that functional testing has been performed on the current version of the TOE, to a degree commensurate with the level of assurance being maintained.

AMA_SIA.1 Security impact analysis

Developer action elements:

AMA_SIA.1.1D The developer security analyst shall, for the current version of the TOE, provide a security impact analysis that covers all changes affecting the TOE as compared with the certified version.

Content and presentation of evidence elements:

AMA_SIA.1.1C The security impact analysis shall identify the certified TOE from which the current version of the TOE was derived.

AMA_SIA.1.2C The security impact analysis shall identify all new and modified TOE components that are categorized as TSP-enforcing.

AMA_SIA.1.3C The security impact analysis shall, for each change affecting the security target or TSF representations, briefly describe the change and any effects it has on lower representation levels.

AMA_SIA.1.4C The security impact analysis shall, for each change affecting the security target or TSF representations, identify all IT security functions and all TOE components categorized as TSP-enforcing that are affected by the change.

AMA_SIA.1.5C The security impact analysis shall, for each change which results in a modification of the implementation representation of the TSF or the IT environment, identify the test evidence that shows, to the required level of assurance, that the TSF continues to be correctly implemented following the change.

AMA_SIA.1.6C The security impact analysis shall, for each applicable assurance requirement in the configuration management (ACM), lifecycle support (ALC), delivery and operation (ADO), and guidance documents (AGD) assurance classes, identify any evaluation deliverables that have changed, and provide a brief description of each change and its impact on assurance.

AMA_SIA.1.7C The security impact analysis shall, for each applicable assurance requirement in the vulnerability assessment (AVA) assurance class, identify which evaluation deliverables have changed and which have not, and give reasons for the decision taken as to whether or not to update the deliverable.

Evaluator action elements:

AMA_SIA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AMA_SIA.1.2E The evaluator shall check, by sampling, that the security impact analysis documents changes to an appropriate level of detail, together with appropriate justifications that assurance has been maintained in the current version of the TOE.

Table 5-2. Tailored Security Assurance Requirements Based on System Risk and Criticality

Security Assurance Class/Family	Security Assurance Component	Low Risk/ Routine System	Moderate Risk/ Essential System	High Risk/ Critical System
Configuration Management:				
Authorization controls	ACM_CAP.3	X	X	X
TOE CM coverage	ACM_SCP.1		X	X
CM automation				ACM_AUT.1
Delivery and Operation:				
Delivery procedures	ADO_DEL.1	X	X	X
Installation, generation, and start-up procedures	ADO_IGS.1	X	X	X
Development:				
Informal functional specification	ADV_FSP.1	X	X	X
Security enforcing high-level design	ADV_HLD.2	ADV_HLD.1	X	X
Informal correspondence demonstration	ADV_RCR.1	X	X	X
Security policy modeling			ADV_SPM.1	ADV_SPM.1
Guidance Documents:				
Administrator guidance	AGD_ADM.1	X	X	X
User guidance	AGD_USR.1	X	X	X
Lifecycle Support:				
Flaw remediation				ALC_FLR.2
Identification of security measures	ALC_DVS.1		X	X
Tests:				
Analysis of coverage	ATE_COV.2	ATE_COV.1	X	X
Testing high-level design	ATE_DPT.1		X	X
Functional testing	ATE_FUN.1	X	X	X
Independent testing – sample	ATE_IND.2	X	X	X
Vulnerability Assessment:				
Covert channel analysis				AVA_CCA.1
Examination of guidance	AVA_MSU.1		X	X
Strength of function evaluation	AVA_SOF.1	X	X	X
Developer vulnerability analysis	AVA_VLA.1	X	X	X
Maintenance of Assurance:				
Assurance maintenance plan		AMA_AMP.1	AMA_AMP.1	AMA_AMP.1
TOE component categorization report		AMA_CAT.1	AMA_CAT.1	AMA_CAT.1
Evidence of assurance maintenance		AMA_EVD.1	AMA_EVD.1	AMA_EVD.1
Security impact analysis		AMA_SIA.1	AMA_SIA.1	AMA_SIA.1
Summary	Standard EAL 3	EAL 2+	EAL 3+	EAL 3+

5.3 Requirements for the IT Environment

This subsection states security requirements for the IT environment in which the TOE will operate. Requirements for the IT environment are stated to reinforce environmental assumptions made in Section 3 of this PP, and in response to security objectives for the environment stated in Section 4 of this PP.

Explicit requirement

FCS_CIF.1 Cryptographic Infrastructure

FCS_CIF.1.1 The IT environment shall support the enterprise-wide cryptographic infrastructure.

Explicit requirement

FPT_ENV.1 Environmental Protection

FPT_ENV.1.1 The IT environment shall monitor and provide protection against natural and manmade environmental threats (fire, flood, humidity, dust, vibration, earthquakes, mud slides, temperature fluctuations, power fluctuations, and so forth).

5.4 Requirements for the Non-IT Environment

This subsection states security requirements for the non-IT environment in which the TOE will operate. Requirements for the non-IT environment are stated to reinforce assumptions made in Section 3 of this PP about the intended use and operation of the TOE and Organizational Security Policies (OSPs).

Explicit requirement

FAU_SAP.1 Security Audit Processing

FAU_SAP.1.1 System security audit records shall be:
(a) reviewed daily by authorized users and administrators
(b) stored online for 7 days
(c) stored offline for 90 days
(d) archived for 2 years

Explicit requirement

FMT_ACR.1 Access Control Rights and Privileges

FMT_ACR.1.1 The security management staff shall implement and/or revoke access control rights and privileges within 10 minutes of being directed to do so by an authorized FAA official.